(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 924 655 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
23.06.1999 Bulletin 1999/25

(51) Int. Cl.[6]: **G07C 9/00**, G07F 7/10

(21) Application number: **98120627.9**

(22) Date of filing: **02.11.1998**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **22.12.1997 US 995328**

(71) Applicant: **TRW Inc.**
Redondo Beach, California 90278 (US)

(72) Inventors:
- **Hsu, Shi-Ping**
  Pasadena, CA 91107 (US)
- **Evans, Bruce W.**
  Redondo Beach, CA 90277 (US)
- **Messenger, Arthur F.**
  Redondo Beach, CA 90278 (US)
- **Zsolnay, Denes L.**
  Rolling Hills Estates, CA 90274 (US)

(74) Representative:
Schmidt, Steffen J., Dipl.-Ing.
Wuesthoff & Wuesthoff,
Patent- und Rechtsanwälte,
Schweigerstrasse 2
81541 München (DE)

(54) Controlled access to doors and machines using fingerprint matching

(57) A system and related method for controlling access to building doors or to machines, such as automatic teller machines (ATMs). The system combines high-speed fingerprint matching with another form of identification carried or memorized by a user (10) of the system. In one disclosed embodiment of the invention, the user (10) carries or wears an identification badge (18) that includes a transponder for sending preliminary identification data to an access controller (14) as the user approaches a door (12) through which access is controlled. The controller (14) uses the preliminary identification data, such as an account number or employee number, to access a fingerprint database (44) and retrieve reference fingerprint data previously stored there during an enrollment procedure. If the user's identification includes a "smart card," the reference fingerprint data may stored in the card instead of in the database (44). The retrieved reference fingerprint data are then compared, in a fingerprint correlator (46), with a subject fingerprint image obtained from the user (10) through a fingerprint sensor (16) located near, or integrated into the door (12). A successful match in the correlator (46) verifies the preliminary identification data and results in access to the door or machine being granted to the user. In another form of the invention, the user carries a conventional machine-readable card, which is placed in a card reader (32) to obtain the preliminary identification data.

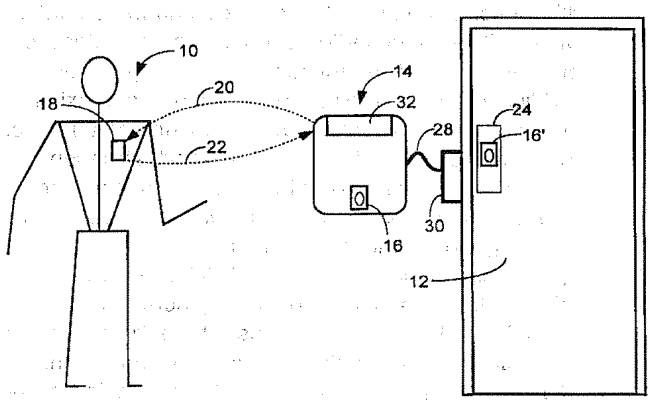

FIG. 1

EP 0 924 655 A2

Description

BACKGOUND OF THE INVENTION

[0001] This invention relates generally to personal identification or verification systems and, more particularly, to systems that automatically verify a person's identity before granting access to a secured area of a company building, or to a secured machine of some kind, such as a bank automatic teller machine (ATM). For building access, employees are typically required to wear or carry identification badges, which are either inspected by security guards or are read by machines installed at access doors. Access to some areas of buildings may also require the employee to key in a lock combination, or supply a secret password.

[0002] Access to an ATM also requires an identification card, which is scanned by the machine to determine the identity of the customer who was issued the card. In an effort to ensure that the person presenting the card is the customer to whom it was issued, a personal identification number (PIN) must also be entered into the machine. Access to highly secured computer systems presents similar problems and usually requires some form of identification used in conjunction with a secret code number or password.

[0003] The principal weakness of systems of the general type described above is that identification cards may be lost or stolen, and secret codes may be stolen, guessed or determined by trial and error. Accordingly, there has been a trend toward systems that obviate the need to carry identification cards or to memorize secret codes or passwords.

[0004] Fingerprint matching falls into this category and has been used or proposed for building access, but has not been widely adopted because of the need for relatively expensive computer equipment to perform the matching process to a desired level of precision. In the past, fingerprint matching systems have been relatively slow. Even with the availability of high-speed computer processors, a fingerprint matching system that must compare a sensed fingerprint image with many possible stored reference images will not operate fast enough to provide rapid access to a building.

[0005] Accordingly, the need still exists for a system of building and machine access that avoids the pitfalls of the prior art techniques. The present invention satisfies this need.

SUMMARY OF THE INVENTION

[0006] The present invention resides in a combination of fingerprint matching and a carried form of personal identification, for access to buildings or machines such as automatic teller machines (ATMs). Briefly, and in general terms, the system of the invention comprises means for inputting a preliminary identification of a user of the system; a fingerprint database containing reference fingerprint data for every user of the system, in association with an identification of the user; means for retrieving from the fingerprint database reference fingerprint data corresponding to the preliminary identification of the user; a fingerprint sensor for generating a fingerprint image of the user prior to granting access; and a fingerprint correlator for comparing the subject fingerprint image with the retrieved reference fingerprint data, and generating a match signal if there is a match to within a desired degree of accuracy. The match signal is used to grant the user access to the door or machine.

[0007] In one embodiment of the invention, the means for inputting a preliminary identification includes means for reading an identification medium carried by each user and having a transponder capable of transmitting identification data in response to receipt of a polling signal; and a polling transceiver for sending polling signals periodically and receiving any response signals from a transponder carried by a user approaching the secured building or machine. In another embodiment, the identification medium carried by each user includes a machine readable card; and the means for reading the identification medium includes a card reader capable of reading the machine readable card to extract preliminary identification data.

[0008] As used to provide access to a secured building, the system further comprises a door release actuator triggered by the match signal. Preferably, the fingerprint sensor is integrated into the door for convenience of use.

[0009] As used to provide access to a bank automatic teller machine (ATM), the system's means for reading an identification medium includes a bank card reader integral with the ATM. The fingerprint sensor is also integrated into the ATM.

[0010] The invention may also be defined in terms of a method for controlling access to a secured building or machine, comprising the steps of reading preliminary identification data supplied by a user seeking access; sensing the user's fingerprint prior to granting access, and generating a fingerprint image; retrieving from a fingerprint database reference fingerprint data corresponding to the preliminary identification data; comparing the reference fingerprint data with the subject fingerprint image to verify the preliminary identification data and, if there is match, generating a match signal; and granting access to the secured building or machine if a match signal is generated.

[0011] In a preferred form of the method, the identification medium carried by each user includes a transponder, and the step of reading preliminary identification data includes transmitting a polling signal, receiving the polling signal in the transponder, and transmitting from the transponder a reply that includes user identification data. In an alternative form of the method, the identification medium carried by each user includes a machine-readable card, and the step of reading data from an identification medium includes reading

data from a card reader in which the machine-readable card is placed by the user. If the machine-readable card is a "smart card," it may hold its own reference fingerprint data as well as preliminary identification data.

[0012] As used to provide access to a protected building, the method of granting access includes unlocking a door to the building, and the step of sensing the user's fingerprint is performed by a sensor integrated into the door for convenience of use. As used to provide access to a machine, the method step of reading data from an identification medium includes reading an identity card in the machine.

[0013] It will be appreciated from the foregoing summary that the present invention represents a significant advance in techniques for controlling access to secured buildings and machines. In particular, the invention provides a high level of security because of its use of fingerprint matching, but does not sacrifice speed or convenience of operation because preliminary identification is provided by the user and fingerprint matching can, therefore, be achieved rapidly. In the preferred form of the invention as used for building access, the combination of fingerprint matching and radio-frequency identification transponders allows users to pass rapidly through a controlled door by simply placing a finger momentarily on a sensor that can be integrated into the door structure. Other aspects and advantages of the invention will become apparent from the following more detailed description, taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014]

FIG. 1 is diagrammatic view showing one technique for obtaining access to a secured building in accordance with the present invention;

FIG. 2 is a block diagram showing the principal components of the invention as used in the technique shown in FIG. 1;

FIG. 3 is a block diagram similar to FIG. 2, but as used for access to an automatic teller machine (ATM) or other machine; and

FIG. 4 is a block diagram showing a fingerprint enrollment process as used in either of the systems of FIGS. 2 and 3.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0015] As shown in the drawings for purposes of illustration, the present invention pertains to a system for controlling access to secured building or machines. In the past, the use of identification cards or badges, in possible combination with secret codes or passwords, has not been reliable because of the possibility of theft of the cards and codes.

[0016] In accordance with the present invention, a high-speed fingerprint matching device is used in conjunction with a personal identification medium carried by each user seeking access to a building or machine. The personal identification medium provides a preliminary identity of the user and the fingerprint matching device provides rapid verification or confirmation of the identity.

[0017] FIG. 1 shows a user, indicated by reference numeral 10, approaching a door 12 to a secured building. An access control unit 14 is installed near the door 12 and includes an integral fingerprint sensor 16. The user 10 is shown wearing an identification badge 18. In accordance with a preferred embodiment of the invention, the access control unit 14 transmits polling signals, indicated by line 20, and the badge 18 includes an integral transponder, which receives the polling signals and transmits a response that includes a coded employee number or, more generally, a user number, as indicated by line 22.

[0018] When the user 10 reaches the door, he or she places a finger on the fingerprint sensor 16. An alternative location for the sensor is, as indicated at 16', integral a push plate 24 on an inwardly opening door, or beneath a pull handle (not shown) on an outwardly opening door. The user has only to pause a fraction of a second while fingerprint verification takes place. Then the access control unit 14 sends a control signal over line 28 to a door release actuator 30, which unlocks the door 12 and allows the user 10 to enter. The access control unit 14 also includes an integral card reader 32, for use by those that do not have a transponder badge 28, or whose badge is not working for some reason. Transponder badge technology, sometimes known as RF-ID (radio-frequency identification), has been discussed in the technical literature.

[0019] An alternative to the use of a badge 28 is to have each user 10 enter an identification code in a keypad (not shown) near the door 12. The preliminary identification is, in effect, memorized and supplied by the user 10 instead of being stored in the badge 28. Verification is still performed by fingerprint matching.

[0020] FIG. 2 shows the principal components of the access control unit 14 in block diagram form, including an identification polling transceiver 40, a door controller 42, a fingerprint database 44, and a fingerprint correlator 46. The polling transceiver 40 continually transmits polling signals, indicated by line 20. As the user 10 approaches, his or her badge 18 detects the polling signal and transmits a reply signal that includes the user's identification number or user number, as indicated by line 22. The user number is forwarded to the door controller 42, over line 48, and, as indicated by line 50, is used to access the fingerprint database 44. The database is basically a table that associates each user number with a stored fingerprint image, or with selected distinctive attributes or features of the user's fingerprint image. The database may also contain other information about the user, such as a history of access to the

door 12, but only the user's stored fingerprint image is of concern to the invention. In case multiple users approach the door simultaneously, means must be provided to prevent interference between the signals from each transponder, and to select the fingerprint of the person who will next try to enter the door 12. This can be achieved simply by limiting the transmitted signal strength of the polling transceiver 40 and badge transponders 18, so that the exchange of signals between transponder and transceiver occurs only when they are in close proximity. Alternatively or additionally, standard signal multiplexing techniques (based on time, frequency or modulation diversity) could be used to eliminate interference, and the strength of the transponder signal received at the transceiver could be used to select the closest transponder.

[0021] At about the same time that the door controller 42 retrieves a reference fingerprint from the database 44, the controller also issues a "start" command to the fingerprint correlator 46, as indicated by line 52. The fingerprint sensor 16 is activated and scans the user's fingerprint. The correlator 46 then rapidly compares the subject fingerprint from the sensor 16, received over line 54, with the reference fingerprint features received from the database 44 over line 56. If the correlator 46 determines that there is a match, a match signal is transmitted to the door controller 42 over line 58, and the controller generates an "open" signal on line 28 to the door release actuator 30.

[0022] Like most automated secured entry systems, the invention does not prevent the practice of "tailgating," where another person follows the one who has been authorized to enter the doorway. This problem can be addressed in other ways, such as by sounding an alarm upon the detection of multiple entries, using photo-detectors or similar devices.

[0023] The fingerprint correlator 46 performs the matching function very rapidly by using special-purpose hardware in the form of an application-specific integrated circuit (ASIC), which employs a high degree of parallel processing to search an entire fingerprint image for instances of distinctive reference features that have been previously stored in the fingerprint database 44. A specific form of the fingerprint correlator that can achieve the desired speed of matching is disclosed in a patent application by Bruce W. Evans et al., entitled "Fingerprint Feature Correlator," filed concurrently with this application. The Evans et al. patent application is hereby incorporated by reference into this specification. A correlator constructed in accordance with the principles described in the Evans et al. specification is capable of verifying a user's identity in less than a second, and closer to half a second if only one reference fingerprint image has to be compared with a sensed fingerprint image

[0024] FIG. 3 is a diagram similar to FIG. 2, but showing the principal components of a system used to access a computer 60, such as a bank automatic teller machine (ATM). Instead of the door controller 42, the corresponding component in FIG. 3 is an access controller 42', and instead of the polling transceiver 40 this system has a bank card reader 62 or a similar device for reading some type of identification card. The card may be encoded with data using a magnetic stripe, bar codes, or any other means. Alternatively, the card may be a "smart card" that includes an electronically readable memory. The user places his or her card in the reader 62, which retrieves an account number or other type of identification unique to the user, and passes this data to the access controller 42' over line 48. As in the door entry system of FIG. 2, the access controller 42' uses the account number, on line 50, to access the fingerprint database 44 and obtain a user reference fingerprint on line 56 from the database. The controller 42' also sends a "start" signal on line 58 to the fingerprint correlator 46, which compares the reference fingerprint with a subject fingerprint image supplied from the sensor 16 over line 54. If the correlator 46 finds a match, the correlator sends a signal over line 58 to the access controller 42', which transmits an appropriate signal to the computer 60 on line 28, indicating that access has been granted. In the case of an ATM machine, the computer 60 initiates a dialog with the user, who may then conduct banking transactions, such as cash withdrawal or deposit transactions. If the computer 60 is for some non-banking purpose, the grant of access may be for any defined purpose, such as the authorization to read from or write to files under control of the computer.

[0025] In the machine access application of the invention, the use of fingerprint matching in conjunction with a conventional bank card or other identification card provides a higher level of security without the need to memorize secret codes or passwords. Door or building access using the technique of the invention has the same general advantage: a higher level of security, without the need for secret codes or passwords, and yet without sacrificing speed or convenience or access. When used in conjunction with automatic badge sensing systems, like RF-ID, the invention provides high security with virtually no inconvenience or delay to the user. If "smart card" technology is used for door or machine access, the card may also be used to store fingerprint reference data for the user. Fingerprint matching at the door or machine would then match the sensed fingerprint image with fingerprint reference data read from the user's card. The need to maintain potentially large fingerprint databases at the door would then be avoided.

[0026] FIG. 4 illustrates an enrollment procedure that is required for any of the configurations described above. It has been assumed in the foregoing description that the fingerprint database 44 contains reference fingerprint image data for each user, employee, or customer using the system, and that the reference fingerprint data are associated with corresponding user numbers, or employee or customer account numbers.

The enrollment procedure requires that each user enroll by presenting a finger to the fingerprint sensor 16, which generates a fingerprint image for a fingerprint enrollment analyzer 64. At the same time, the user's identity has to be independently verified, by some means other than fingerprint matching, as indicated in block 66, and the user also presents an account number, employee number or similar identity number. If the user does not have such a number, one is assigned at this stage. The account number is stored in the database 44 in association with the user's fingerprint image data. The fingerprint correlator 46 described in the patent specification of Bruce W. Evans et al. referred to above, also includes an analysis section that extracts distinctive features from a fingerprint image, in the form of reference "patches" of the image that contain one or more distinctive bifurcations of ridges or valleys in the fingerprint image. In the system of the present invention, it is these reference patches, and their positions, that are stored in the fingerprint database 44, or directly on the user's identification card, if "smart card" technology is used, for later retrieval and use in the correlator 46.

[0027] It will be appreciated from the foregoing that the present invention represents a significant advance in the field of automatic security systems controlling access to buildings or machines. In particular, the combination of an identity medium, such as a badge or card, to identify the user, and fingerprint matching to verify the identity, results in a highly secure but highly convenient approach to access control. It will also be appreciated that, although specific embodiments of the invention have been described in detail for purposes of illustration, various modifications may be made without departing from the spirit and scope of the invention. Accordingly, the invention should not be limited except as by the appended claims.

Claims

1. A system for controlling access to a secured building or machine, the apparatus comprising:

   means for inputting a preliminary identification of a user of the system;
   a fingerprint database containing reference fingerprint data for every user of the system, in association with an identification of the user;
   means for retrieving from the fingerprint database reference fingerprint data corresponding to the preliminary identification of the user;
   a fingerprint sensor for generating a subject fingerprint of the user prior to granting access; and
   a fingerprint correlator for comparing the subject fingerprint image with the retrieved reference fingerprint data, and generating a match signal if there is a match to within a desired degree of accuracy;
   wherein the match signal is used to grant access to the door or machine.

2. A system as defined in claim 1, wherein:

   the means for inputting a preliminary identification includes means for reading an identification medium carried by each user and having a transponder capable of transmitting identification data in response to receipt of a polling signal; and
   the means for reading an identification medium includes a polling transceiver for sending polling signals periodically and receiving any response signals from a transponder carried by a user approaching the secured building or machine.

3. A system as defined in claim 1, wherein:

   each user carries a machine readable card; and
   the means for inputting a preliminary identification includes a card reader capable of reading the machine readable card to extract preliminary identification data.

4. A system as defined in claim 1, wherein:

   the system provides access to a secured building; and
   the system further comprises a door release actuator triggered by the match signal.

5. A system as defined in claim 4, wherein the fingerprint sensor is integrated into the door for convenience of use.

6. A system as defined in claim 1, wherein:

   the system provides access to a bank automatic teller machine (ATM); and
   the means for inputting a preliminary identification includes a bank card reader integral with the ATM; and
   the fingerprint sensor is also integrated into the ATM.

7. A method for controlling access to a secured building or machine, the method comprising:

   reading preliminary identification data supplied by a user seeking access;
   sensing the user's fingerprint prior to granting access, and generating a subject fingerprint image;
   retrieving from a fingerprint database reference

fingerprint data corresponding to the preliminary identification data;

comparing the reference fingerprint data with the subject fingerprint image to verify the preliminary identification data and, if there is match, generating a match signal; and

granting access to the secured building or machine if a match signal is generated.

8. A method as defined in claim 7, wherein:

the step of reading preliminary identification data includes transmitting a polling signal to a transponder carried by the user, receiving the polling signal in the transponder, transmitting from the transponder a reply that includes user identification data.

9. A method as defined in claim 7, wherein:

each user carries a machine-readable card; and

the step of reading preliminary identification data includes reading data from a card reader in which the machine-readable card is placed by the user.

10. A method as defined in claim 7, wherein:

the method provides access to a protected building; and

the step of granting access includes unlocking a door to the building.

11. A method as defined in claim 10, wherein the step of sensing the user's fingerprint is performed by a sensor integrated into the door for convenience of use.

12. A method as defined in claim 7, wherein:

the method provides access to a protected machine; and

the step of reading preliminary identification data includes reading an identity card in the machine.

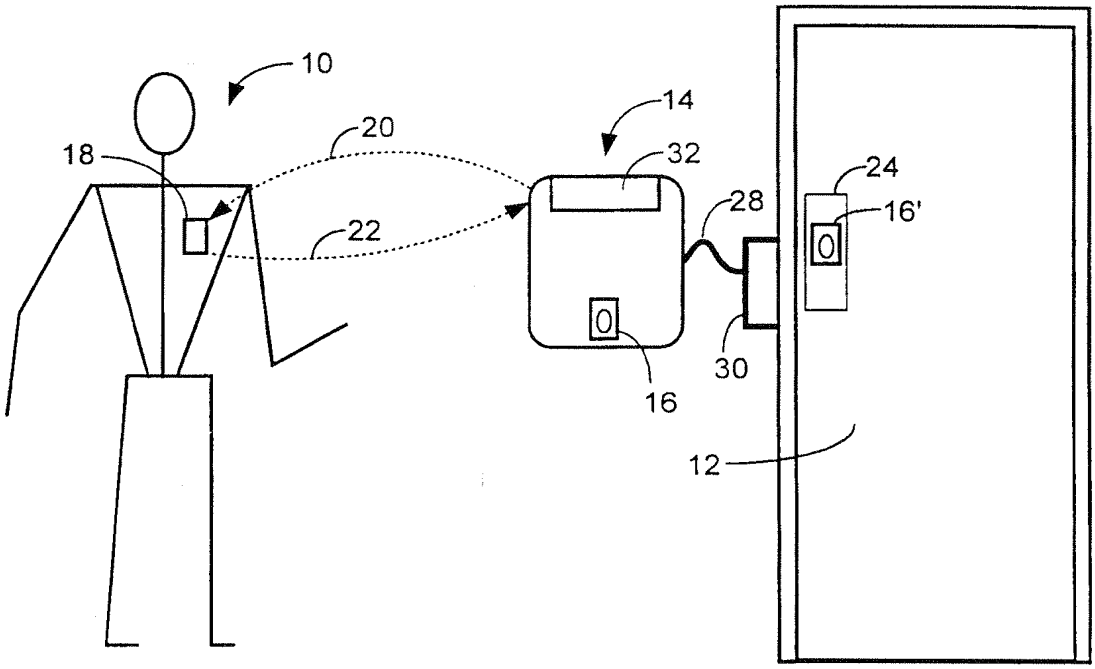

FIG. 1

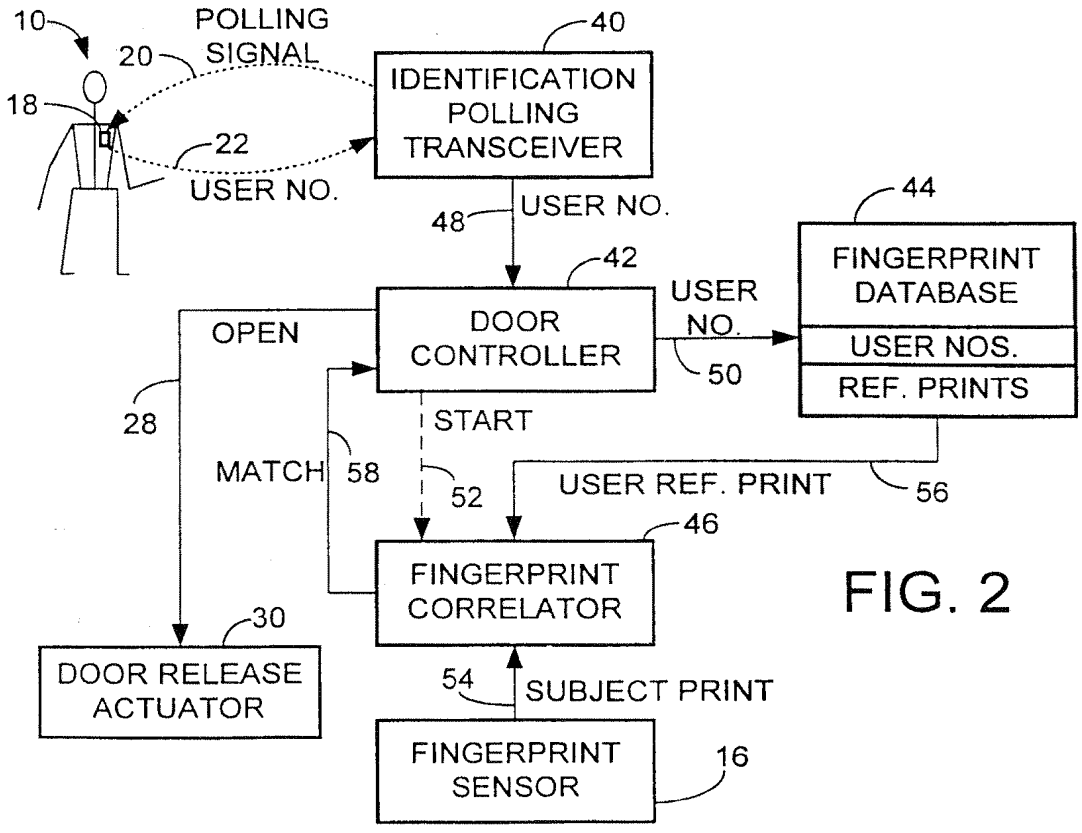

FIG. 2

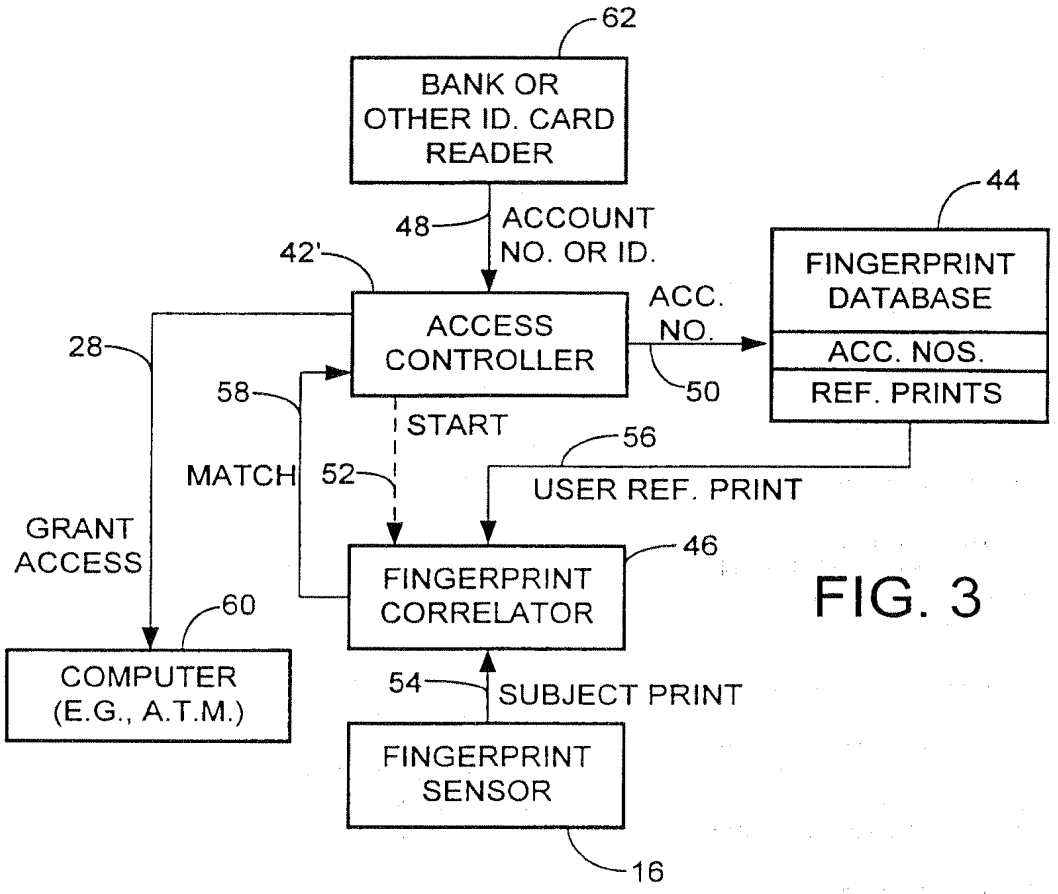

FIG. 3

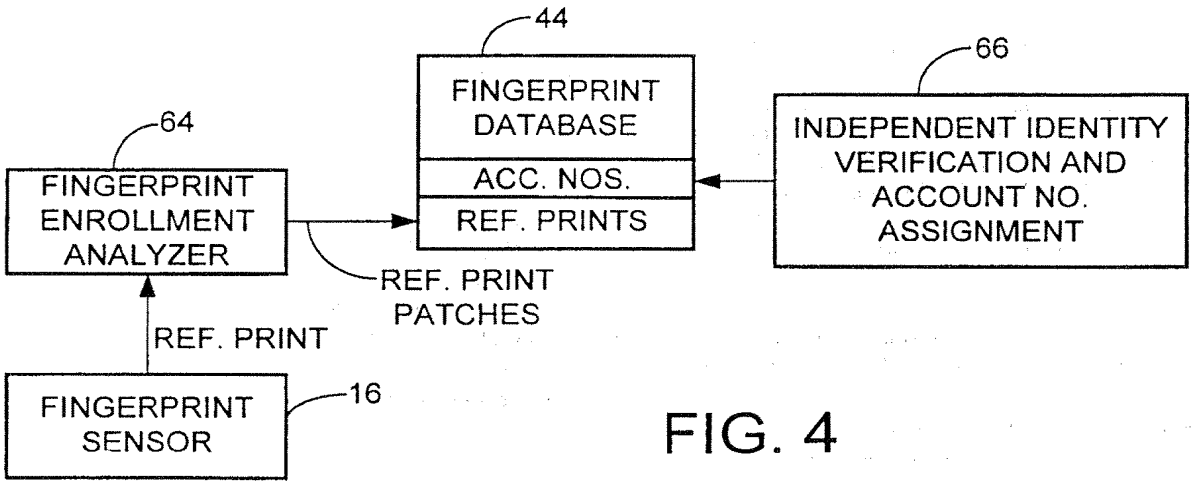

FIG. 4

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 924 655 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
01.03.2000 Bulletin 2000/09

(43) Date of publication A2:
23.06.1999 Bulletin 1999/25

(21) Application number: **98120627.9**

(22) Date of filing: **02.11.1998**

(51) Int. Cl.[7]: **G07C 9/00**, G07F 7/10

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **22.12.1997 US 995328**

(71) Applicant: **TRW Inc.**
Redondo Beach, California 90278 (US)

(72) Inventors:
- **Hsu, Shi-Ping**
  Pasadena, CA 91107 (US)
- **Evans, Bruce W.**
  Redondo Beach, CA 90277 (US)
- **Messenger, Arthur F.**
  Redondo Beach, CA 90278 (US)
- **Zsolnay, Denes L.**
  Rolling Hills Estates, CA 90274 (US)

(74) Representative:
Schmidt, Steffen J., Dipl.-Ing.
Wuesthoff & Wuesthoff,
Patent- und Rechtsanwälte,
Schweigerstrasse 2
81541 München (DE)

(54) Controlled access to doors and machines using fingerprint matching

(57) A system and related method for controlling access to building doors or to machines, such as automatic teller machines (ATMs). The system combines high-speed fingerprint matching with another form of identification carried or memorized by a user (10) of the system. In one disclosed embodiment of the invention, the user (10) carries or wears an identification badge (18) that includes a transponder for sending preliminary identification data to an access controller (14) as the user approaches a door (12) through which access is controlled. The controller (14) uses the preliminary identification data, such as an account number or employee number, to access a fingerprint database (44) and retrieve reference fingerprint data previously stored there during an enrollment procedure. If the user's identification includes a "smart card," the reference fingerprint data may stored in the card instead of in the database (44). The retrieved reference fingerprint data are then compared, in a fingerprint correlator (46), with a subject fingerprint image obtained from the user (10) through a fingerprint sensor (16) located near, or integrated into the door (12). A successful match in the correlator (46) verifies the preliminary identification data and results in access to the door or machine being granted to the user. In another form of the invention, the user carries a conventional machine-readable card, which is placed in a card reader (32) to obtain the preliminary identification data.

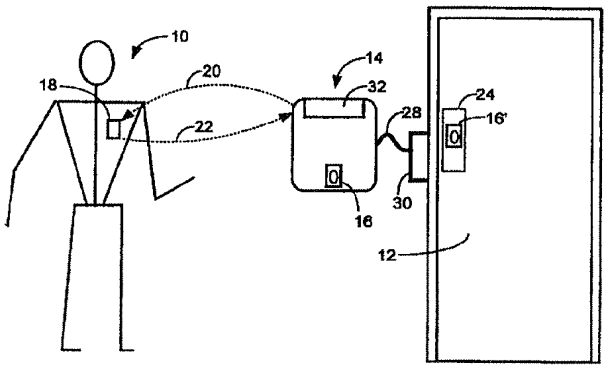

FIG. 1

EP 0 924 655 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 12 0627

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	US 4 995 086 A (LILLEY ROBERT M ET AL) 19 February 1991 (1991-02-19)	1,3,4,6, 7,9,10, 12	G07C9/00 G07F7/10
Y	* column 1, line 61 - column 3, line 9 * * column 5, line 3 - line 13 * * figures *	2,5,8,11	
X	US 4 805 223 A (DENYER PETER B) 14 February 1989 (1989-02-14) * column 1, line 45 - column 2, line 3 * * column 3, line 35 - line 59 * * column 6, line 62 - column 7, line 55; figures *	1,3,4,6, 7,9,10, 12	
Y	EP 0 393 784 A (NEDAP NV) 24 October 1990 (1990-10-24) * column 1, line 1 - line 12 * * column 3, line 17 - column 4, line 31 * * column 6, line 7 - line 46 * * claim 1 *	2,8	
Y	WO 93 18486 A (RUYVEN LODEWIJK JOHAN VAN) 16 September 1993 (1993-09-16) * abstract * * claims 1,11-13; figures 1,2 *	5,11	TECHNICAL FIELDS SEARCHED (Int.Cl.6) G07C G07F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	11 January 2000	Teutloff, H

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 12 0627

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

11-01-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4995086 A	19-02-1991	EP 0244498 A	11-11-1987
		AT 64484 T	15-06-1991
		JP 62278685 A	03-12-1987
US 4805223 A	14-02-1989	EP 0218668 A	22-04-1987
		WO 8606527 A	06-11-1986
		GB 2174831 A,B	12-11-1986
		JP 62502575 T	01-10-1987
EP 0393784 A	24-10-1990	NL 8900949 A	16-11-1990
		CA 2014687 A	17-10-1990
WO 9318486 A	16-09-1993	NL 9200439 A	01-10-1993
		DE 69322635 D	28-01-1999
		DE 69322635 T	22-07-1999
		EP 0638190 A	15-02-1995
		JP 7504524 T	18-05-1995
		US 5729334 A	17-03-1998

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82